7 Steps to Strengthen Your Security Program Today

Managing a security program in today's ever-changing cyber threat landscape is no small feat. Cybersecurity programs must be continually evaluated and should evolve as cyber threats and company risk changes. This checklist is designed to get you started and will help you gain traction for future program improvements.

1. Assess your current security program.

Start by choosing a framework for your security program and evaluate from a business standpoint to determine if the benefit of a security control or practice outweighs the cost.

2. Identify what data you have and where it lives.

Identify what data your company has stored, created, or controlled to understand your cybersecurity and data protection priorities. Then, identify whether sensitive data is stored in cloud services, on hard drives, or in file servers as this changes your strategy to protect it.

3. Implement & enforce policies to combat insider threat.

Policies are needed to combat the human element of cybersecurity. An insider threat isn't always a nefarious actor out to steal company data; it can be a well-meaning employee who unknowingly shares a document in an insecure way and exposes data.

4. Implement a security awareness training program.

Security awareness training can teach an employee to recognize the signs of phishing emails and may prevent the employees and the company from falling victim to a phishing attack.

5. Talk to your IT team for multi-factor authentication & anti-phishing measures.

Multi-factor authentication (MFA) should be used to prevent unauthorized access to business critical systems and anti-phishing measures should be taken to protect corporate email systems.

6. Implement third-party vendor risk management program.

Implement a third-party risk management program in which new and existing service providers must show proof of their internal security program practices and controls, before allowing access into a corporate system.

7. Implement onboarding & offboarding policies that integrate HR & IT.

Access to systems should be approved by HR (to prevent extra accounts and backdoors from being created without company knowledge), and departed employees should be immediately deprovisioned from all systems.

GRA QUANTUM

graquantum.com | info@graquantum.com

About GRA Quantum

Our Approach

We exist because it takes a whole new set of rules to respond to today's problems and anticipate tomorrow's solutions. It requires a team experienced in the highest echelons of the private sector and government intelligence – a team comprised of people who care deeply about protecting society. And it demands a holistic understanding of the technical, physical, and human elements behind security threats.

Our Core Services

Managed Security Services

By combining advanced technology with unparalleled human expertise within our Security Operations Center, our MSS provides the necessary functions to respond to the evolving threat landscape, including:

Monitoring & Alerting

Incident Handling

Threat Hunting

Professional Services

From device management to asset tracking and endpoint protection, we'll assess and build the right security environment for your unique needs.

Plan & Assess

- Security Risk Assessment
- Penetration Tests & Vulnerability Management

Prepare & Protect

- Insider Threat Programs
- Cybersecurity training
- Secure Communications
- Secure Travel Program

Readiness & Response

- Tabletop Exercises
- Incident Response
- Digital Forensics
- Insider Threat Investigations